

On the Greatest Common Divisor of Binomial Coefficients $\binom{n}{q}, \binom{n}{2q}, \binom{n}{3q}, \dots$

Carl McTague

ABSTRACT. Every binomial coefficient aficionado¹ knows that the greatest common divisor of the binomial coefficients $\binom{n}{1}, \binom{n}{2}, \dots, \binom{n}{n-1}$ equals p if $n = p^i$ for some $i > 0$ and equals 1 otherwise. It is less well known that the greatest common divisor of the binomial coefficients $\binom{2n}{2}, \binom{2n}{4}, \dots, \binom{2n}{2n-2}$ equals (a certain power of 2 times) the product of all odd primes p such that $2n = p^i + p^j$ for some $i \leq j$. This note gives a concise proof of a tidy generalization of these facts.

THEOREM 1 ([Ram09]). For any integer $n > 1$ and any prime p :

$$\text{GCD}_{0 < k < n} \binom{n}{k} = \begin{cases} p & \text{if } n = p^i \text{ for some } i > 0 \\ 1 & \text{otherwise} \end{cases}$$

THEOREM 2 (Lemma 12 of [McT14a]). For any integer $n > 1$ and any prime $p > 2$:

$$\text{ord}_p \left[\text{GCD}_{0 < k < n} \binom{2n}{2k} \right] = \begin{cases} 1 & \text{if } 2n = p^i + p^j \text{ for some } 0 \leq i \leq j \\ 0 & \text{otherwise} \end{cases}$$

where $\text{ord}_p(m)$ is the highest power of p dividing an integer m .

REMARK. For a given integer $n > 1$, at most one prime p divides the GCD in Theorem 1. But more than one prime can divide the GCD in Theorem 2, which is why ord_p is used to state it. For example, if $n = 3$ then $2n = 3^1 + 3^1 = 5^0 + 5^1$ and indeed $\text{GCD}_{0 < k < 3} \binom{6}{2k} = 15 = 3 \cdot 5$. In fact, more than two primes can divide: if $n = 15$ then $2n = 3^1 + 3^3 = 5^1 + 5^2 = 29^0 + 29^1$ and indeed $\text{GCD}_{0 < k < 15} \binom{30}{2k} = 435 = 3 \cdot 5 \cdot 29$.

These theorems are special cases of a (new) more general result:

THEOREM Q. For any integers $n > q > 0$, and for any prime p congruent to 1 modulo q :

$$\text{ord}_p \left[\text{GCD}_{0 < k < n/q} \binom{n}{qk} \right] = \begin{cases} 1 & \text{if } \alpha_p(n) \leq q \\ 0 & \text{otherwise} \end{cases}$$

where $\alpha_p(n)$ is the sum of the digits of the base- p expansion of n , equivalently the smallest integer r such that $n = p^{i_1} + \dots + p^{i_r}$ for integers $0 \leq i_1 \leq \dots \leq i_r$.

REMARK. Since p is congruent to 1 modulo q , the inequality $\alpha_p(n) \leq q$ is equivalent to the equality $\alpha_p(n) = s$ where s is the unique integer in the range $0 < s \leq q$ congruent to n modulo q . (Indeed, since p is congruent to 1 modulo q , so is each power p^i , so $\alpha_p(n)$ is congruent to n modulo q .) For example, for $n > 1$:

$$\text{ord}_p \left[\text{GCD}_{0 < k < n} \binom{qn}{qk} \right] = \begin{cases} 1 & \text{if } \alpha_p(qn) = q \\ 0 & \text{otherwise} \end{cases}$$

¹The author regards himself less *aficionado* than *espontáneo*, cf [Bur01, p. 52].

while:

$$\text{ord}_p \left[\text{GCD}_{0 < k \leq n} \binom{qn+1}{qk} \right] = \begin{cases} 1 & \text{if } \alpha_p(qn+1) = 1 \\ 0 & \text{otherwise} \end{cases}$$

When $q = 2$, the former is Theorem 2, while the latter a priori extends Theorem 2. However, due to the symmetry of Pascal's triangle $\binom{n}{k} = \binom{n}{n-k}$, this extension can already be deduced from Theorem 1.

REMARK. The hypothesis that p is congruent to 1 modulo q was chosen for its balance of simplicity and generality, and is used in two different ways in the proof of Theorem Q (below). It can be weakened, for example, to p and q being relatively prime and $p^{i_1} \equiv \dots \equiv p^{i_r} \pmod{q}$. (In the last paragraph of the proof, replace $(p-1)p^{i_r-1}$ with qp^{i_r-1} when $p^{i_1} \equiv \dots \equiv p^{i_r} \not\equiv 1 \pmod{q}$.) But it cannot be eliminated altogether since, for example, $\text{ord}_2 [\text{GCD}_{0 < k < 2} \binom{6}{3k}] = \text{ord}_2(20) = 2$.

REMARK. A different generalization of Theorem 1 is obtained in [JOS85] by determining the greatest common divisor of $\binom{n}{r}, \binom{n}{r+1}, \dots, \binom{n}{s}$ for any $r \leq s \leq n$.

The proof of Theorem Q relies on:

KUMMER'S THEOREM ([Kum52], cf [Gra97, §1]). For any integers $0 \leq k \leq n$ and any prime p :

$$\text{ord}_p \left[\binom{n}{k} \right] = \# \{ \text{carries when adding } k \text{ to } n-k \text{ in base } p \}$$

In particular, it relies on the following consequence of Kummer's theorem:

LEMMA 3. *Given two integers $0 \leq k \leq n$, write their base- p expansions in the form:*

$$k = p^{j_1} + \dots + p^{j_s} \qquad n = p^{i_1} + \dots + p^{i_r}$$

with r and s minimal, $i_1 \leq \dots \leq i_r$ and $j_1 \leq \dots \leq j_s$. Then $\text{ord}_p \left[\binom{n}{k} \right] = 0$ if and only if (j_1, \dots, j_s) is a subsequence of (i_1, \dots, i_r) .

PROOF OF LEMMA 3. By Kummer's theorem, $\text{ord}_p \left[\binom{n}{k} \right] = 0$ if and only if there are no carries when adding k to $n-k$ in base p . This happens if and only if each base- p digit of k is \leq the corresponding base- p digit of n . And this in turn is equivalent to (j_1, \dots, j_s) being a subsequence of (i_1, \dots, i_r) . \square

PROOF OF THEOREM Q. To begin, note that for any set S of integers:

$$\text{ord}_p [\text{GCD } m] = \min_{m \in S} \text{ord}_p(m)$$

So this order equals 0 if there is an integer m in S with $\text{ord}_p(m) = 0$. Similarly, this order equals 1 if (a) for every integer m in S , $\text{ord}_p(m) > 0$ and (b) there is an integer m in S with $\text{ord}_p(m) = 1$.

Now, write the base- p expansion of n in the form:

$$n = p^{i_1} + \dots + p^{i_r}$$

with r minimal and $i_1 \leq \dots \leq i_r$.

If $r > q$ then by Lemma 3:

$$\text{ord}_p \left[\binom{p^{i_1} + \dots + p^{i_r}}{p^{i_1} + \dots + p^{i_q}} \right] = 0$$

Since p is congruent to 1 modulo q , so is each power p^i , so $p^{i_1} + \dots + p^{i_q}$ is divisible by q , and it follows that $\text{ord}_p [\text{GCD}_{0 < k < n/q} \binom{n}{qk}] = 0$.

If $r \leq q$ then $p^{j_1} + \dots + p^{j_s}$ is not divisible by q for any nonempty proper subsequence (j_1, \dots, j_s) of (i_1, \dots, i_q) . Therefore, by Lemma 3, $\text{ord}_p \left(\binom{n}{qk} \right) > 0$ for any k with $0 < qk < n$. So $\text{ord}_p [\text{GCD}_{0 < k < n/q} \binom{n}{qk}] > 0$.

The largest exponent i_r must be > 0 since otherwise $n = p^0 + \dots + p^0 = r \leq q$, and by assumption $n > q$. Since r is minimal, it equals the sum $\alpha_p(n)$ of the base- p digits of n , so this sum is by assumption $\leq q$. And $q < p$ since p is prime and congruent to 1 modulo q . It follows that the $(i_r - 1)$ st base- p digit of n is less than $p - 1$. So there is exactly one carry when adding $(p - 1)p^{i_r - 1}$ to $n - (p - 1)p^{i_r - 1}$. By Kummer's theorem then:

$$\text{ord}_p \left[\binom{p^{i_1} + \dots + p^{i_r}}{(p - 1)p^{i_r - 1}} \right] = 1$$

Since p is congruent to 1 modulo q , $(p - 1)p^{i_r - 1}$ is divisible by q , and it follows that $\text{ord}_p[\text{GCD}_{0 < k < n/q} \binom{n}{qk}] = 1$. \square

Thanks to Doug Ravenel, David Gepner and Marcus Zibrowius for helpful conversations. Thanks to the referee who suggested generalizing an earlier version of Theorem Q. Thanks to Günter Ziegler for pointing out [Ram09]. Thanks to the villains [McT14b] who haunt the Hopkins mathematics department for helping inspire this work.

References

- [Bur01] William Burroughs, *Naked Lunch : the restored text*, Grove Press, New York, 2001.
- [Gra97] Andrew Granville, Arithmetic properties of binomial coefficients, I, Binomial coefficients modulo prime powers. *Organic mathematics* (Burnaby, BC, 1995), Vol. 20 of *CMS Conf. Proc.* 253–276, Amer. Math. Soc., Providence, RI, 1997, www.dms.umontreal.ca/~andrew/Binomial/.
- [JOS85] H. Joris, C. Oestreicher, J. Steinig, The greatest common divisor of certain sets of binomial coefficients, *J. Number Theory* **21** no. 1 (1985) 101–119, [dx.doi.org/10.1016/0022-314X\(85\)90013-7](https://doi.org/10.1016/0022-314X(85)90013-7).
- [Kum52] E. E. Kummer, Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen, *J. Reine Angew. Math.* **44** (1852) 93–146.
- [McT14a] Carl McTague, The Cayley plane and string bordism, *Geom. Topol.* **18** no. 4 (2014) 2045–2078, [dx.doi.org/10.2140/gt.2014.18.2045](https://doi.org/10.2140/gt.2014.18.2045).
- [McT14b] Carl McTague, Binomial coefficients and villainy, 2014, www.mctague.org/carl/blog/2014/12/02/moriarty/.
- [Ram09] B. Ram, Common factors of $\frac{n!}{m!(n-m)!}$, ($m = 1, 2, \dots, n - 1$), *J. Indian Math. Club (Madras)* **1** (1909) 39–43, hdl.handle.net/2027/njp.32101080760422?urlappend=%3Bseq=51.

E-mail address: carl.mctague@rochester.edu

URL: www.mctague.org/carl

MATHEMATICS DEPARTMENT, UNIVERSITY OF ROCHESTER, ROCHESTER, NY 14627, USA